УДК 004.056

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ПРОЦЕСУ ОБРОБКИ РИЗИКІВ

Начовна Д.А., Мартиненко А.А.
Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/,
E-mail:darja.tkacevich@gmail.com

Робота присвячена аналізу методів обробки ризиків, як одного з ключових етапів процесу управління ризиками інформаційної безпеки. Обробка ризиків – складний інформаційномісткий процес, який можливо спростити та зробити структурованим за допомогою систем підтримки прийняття рішення, зокрема стратегічних.

Ключові слова – обробка ризиків, методи обробки ризиків, система підтримки прийняття рішень, інформаційна безпека, управління ризиками інформаційної безпеки.

ВСТУП

Управління ризиками – високе мистецтво. Світова практика показує, що єдина можливість запобігання будь-якої світової кризи та збереження стабільності – оволодіти мистецтвом управління ризиків. Сфера інформаційної безпеки не є виключенням.

Важливими нагальними питаннями в управлінні ризиками інформаційної безпеки залишаються основні його етапи: оцінка ризиків та обробка ризиків. Що цікаво, сьогодні не існує єдиного шаблонного варіанту щодо визначення основних стовпів управління ризиками. Більше того, державні законотворці та регулятори мають тенденцію ускладнювати і без того тернистий пошук ідеального балансу досягнення інформаційної безпеки та пов'язаними з цим перевагами, при цьому зберігаючи правильне інвестування та залишаючись конкурентноспроможними, ефективними, успішними та рентабельними. Подібний баланс кожна організація вимушена шукати індивідуально.

ОБРОБКА РИЗИКІВ

Тож, процес обробки ризиків є одним з головних етапів управління ризиків інформаційної безпеки, метою якого є або максимальне зниження вірогідності реалізації такого, або мінімальна величина збитку, який може понести компанія. На перший погляд може здатись, що достатньо легко можна досягти досить прозорої кінцевої мети. Проте практика показує, що максимальний ефект в обробці ризиків досягається синтезом, і в кожному конкретному випадку, навіть маючи схожі вихідні данні, синтез рішень зовсім не обов'язково буде шаблонним.

Залежно від того, чи відбуватимуться зміни характеристик ризиків, можна виділити регулювання та фінансування ризиків.

До регулювання ризиків відносяться методи, в результати яких відбувається цільова зміна таких характеристик ризику, як ймовірність, наслідки або розкид можливих результатів. Фінансування ризику має на меті компенсацію наслідків реалізації ризику, без зміни його властивостей.

Залежно від того, що буде відбуватись з ризиком після впровадження наступних методів, оцінку ризиків можна розділити на 4 категорії [1] (див. Табл.1):

- прийняття ризику;
- зменшення ризику;
- перекладання ризику;
- уникнення ризику.

Таблиця 1. Класифікація методів обробки ризику

Метод	Що відбувається з ризиком
Прийняття ризику	Ризик продовжує існувати та повністю залишається у даного суб'єкта
Зменшення ризику	Ризик продовжує існувати у даного суб'єкта, проте змінюється (зменшується) його рівень (зазвичай кількісна характеристика)
Перекладання ризику	Ризик продовжує існувати, проте всі або окремі його компоненти передаються іншим особам
Уникнення ризику	Ризик перестає існувати у даного суб'єкта

1. Рішення про прийняття ризику для починаючого високотехнологічного підприємства набагато ймовірніше, аніж для солідної організації стандартної орієнтації. Кожна організація має встановити власні критерії прийняття ризиків, тим самим визначити максимально припустимий залишковий ризик. Всі ризики, що перевищують припустимий залишковий, мають автоматично не прийматись. Іншій ж мають пройти через детальний кількісний та якісний аналіз ризиків.

2. Рішення про зменшення ризиків розглядають завжди першочергово, коли ризик є неприйнятним. Мова йде про зменшення ризику до максимально прийнятного значення шляхом використання механізмів контролю. Останні можна знайти в міжнародних стандартах ISO 27001 та ISO 27002, котрі містять опис та керівництво по застосуванню для кожного з механізмів контролю. Крім стандартів серії ISO 2700x та інших серій, в нагоді можуть бути й інші міжнародні стандарти. Наприклад, німецькі стандарти серії BSI/IT - Baseline Protection Manual.

Вибір механізма контролю, як і будь-який інший вибір, треба обґрунтовувати. Якісним показником економічної доцільності використання того чи іншого методу, його ефективності та реалізує мості може слугувати коефіцієнт повернення інвестицій (ROI), що обчислюється за формулою (1):

$$ROI = (\text{Зменш. середньорічних втрат} - \text{Вартість захисних заходів}) / \text{Вартість захисних заходів}, \quad (1)$$

Якщо коефіцієнт повернення інвестицій від'ємний (ROI<0), це свідчить про те, що засоби захисту

інформації дорожчі безпосередньо за інформацію. В такому разі треба переглянути комплекс захисту.

3. Якщо зменшення ризику до певного рівня є проблематичним, можна використати метод передачі ризику третій стороні. В цьому випадку третьою стороною можуть виступити страхові фірми чи аутсорсингові компанії. При передачі ризику особливу увагу треба звертати на юридичну сторону оформлення, адже від цього залежить своєчасність і повнота виплати в разі настання страхового випадку. Не треба забувати і про залишкові ризики, які не можливо виключити в даному методі. Це пов'язано з тим, що страхування в сфері інформаційної безпеки тільки починає розвиватись в Україні і ще немає чіткого визначення страхового випадку за подією інформаційної безпеки. На сьогоднішній день неможливо застрахувати ризики, пов'язані з технологічними помилками, ризики при реалізації проектів та кібер-ризики.

Для того, щоб в Україні страхування ризиків ІБ мало успішну практику, необхідно подолати наступні етапи становлення:

- створити методологію оцінки рівня збитків від витоку інформації з обмеженим доступом;
- створити власну актуальну і не суперечливу законодавчу базу, котра б детально описувала процес страхування інформаційних ризиків;
- вимоги національних українських документів з інформаційної безпеки повинні бути орієнтовані не тільки на державні структури, а й на бізнес;
- не допускати введення цензури в країні, щоб у міжнародної спільноти створювалося об'єктивне уявлення про ситуацію в Україні, тим самим забезпечити входження України у світовий інформаційний простір.

4. Уникнення ризику є доцільним, коли є можливість відносно безболісної реорганізації бізнесу. Це можуть бути рішення про відмову обробляти певну конфіденційну інформацію, про відмову від деяких запланованих бізнес-активностей або перенесення власних ресурсів з зони ризику. Проте варто пам'ятати принцип ведення бізнесу, коли професійніше – навчитися управляти ризиками, а не шукати можливості уникнути таких.

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ ДЛЯ ПРОЦЕСУ ОБРОБКИ РИЗИКІВ – ПРИНЦИП ТАКСОНОМІЇ

Так, як способи обробки ризиків не є взаємовиключними, а вибір способу синтезу методів обробки ризиків є складним завданням, при цьому границі між основними чотирма методами обробки ризику є досить умовними та тонкими, то є потреба застосовувати систему підтримки прийняття рішення.

Система підтримки прийняття рішення [2] - це інтерактивні автоматизовані інформаційні системи, які допомагають особам, що приймають рішення, використовувати дані та моделі для того, щоб вирішувати неструктуровані та слабко структуровані проблеми (задачі).

В СППР використовують останні рішення в галузі інформаційних технологій: сховища та вітрини даних, OLAP-технології, нейромережі, штучний інтелект, генетичні алгоритми, добування знань (Data Mining).

Існує безліч класифікацій СППР. Та в випадку з аналізом значних обсягів різнорідної інформації, що збираються з різних джерел, краще використовувати стратегічні СППР. Найважливішою метою стратегічних систем підтримки прийняття рішення є пошук найбільш раціональних варіантів розвитку із урахуванням багатофакторного. Головною перевага такої системи - можливість менеджерам компанії обґрунтовувати свої рішення на основі аналізу великих масивів інформації.

Якщо провести аналогію поміж СППР та таксономією [3], то системи підтримки прийняття рішення є простішими в реалізації, при цьому принципи залишаються спільними – класифікація та систематизація складно організованих областей дійсності.

ВИСНОВКИ

Прийняття остаточного рішення в питанні обробки ризиків хибно вважають обов'язком спеціаліста з захисту інформації. Адже відповідальність за вибір тієї чи іншої моделі обробки ризиків можна порівняти з типовим бізнес-рішенням, котре має приймати керівник організації. Зазвичай, подібні рішення є ключовими і ведуть за собою зміни в роботі, а інколи і звичному функціонуванні установи.

Зрозуміло, що попередньо керівник має володіти повною, достовірною, підкріпленою фактами інформацією про наступне:

- наявність та рівень серйозності проблеми;
- наслідки у випадку відсутності будь-якої реакції на виклики;
- запропоновані рішення (обов'язково має бути декілька, так як альтернатива є завжди і керівник має право та обов'язок самостійно обирати);
- наявність і рівень залишкового ризику.

Наступним кроком після прийняття рішення має стати розробка плану обробки ризиків. Створення такого документу, реалізація та контроль за виконанням покладається на спеціаліста з інформаційної безпеки. Найчастіше таким документом слугує «Декларація про застосування механізмів контролю».

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Астахов Александр, Искусство управления информационными рисками. М.: ДМК Пресс, 2010. – 312 с.

2. Бідюк П.І., Гожий О.П., Коршевнюк Л.О., Комп'ютерні системи підтримки прийняття рішень. (Електрон. ресурс) / Спосіб доступу – http://lib.chdu.edu.ua/pdf/posibnuku/313/3.pdf - Заголовок з екрана.

3. Черешкин Д.С., Принципы таксономии угроз безопасности информационных систем. (Електрон. ресурс) / Спосіб доступу – http://www.iso27000.ru - Заголовок з екрана.